imperva

SA Power Networks

Protects web applications and API endpoints with Imperva Application Security

CASE STUDY

THALES
Building a future we can all trust
CYBERSECURITY

SA Power Networks Overview

SA Power Networks is a key player in South Australia's energy industry as the state's sole electricity distributor. It builds, maintains, and upgrades the poles, wires, and substations that deliver power to around 900,000 homes and businesses. In addition, SA Power Networks operates a 24-hour faults and emergencies hotline, maintains street lighting for local councils and government, and takes readings of traditional SA Power Networks' electricity meters.

SA Power Networks

Company: **SA Power Networks**

Founded in: **2012**

Industry: **Energy & Utilities**

Location: **Adelaide, Australia**

Website: sapowernetworks.com.au

Challenges

Safeguarding South Australia's power grid

Energy isn't just about keeping the lights on, it powers lives and sustains businesses. As South Australia's singular electricity provider, disruption to SA Power Networks is simply not an option. As a significant utility to the state and country, the company was constantly under threat. "We are required every day for people to live their lives. So you've got to really put the customer first," said Nathan Morelli, Head of Cybersecurity and IT Resilience at SA Power Networks.

More than seven years ago, SA Power Networks deployed Imperva Cloud WAF to protect its web applications as a pivotal component of its cybersecurity strategy. This was crucial to keep power up and running, and the employees needed to continue to use their time to problem solve for their end users, not problem solve how to use necessary applications. The platform helped to differentiate between increased activity due to DDoS attacks vs. legitimate customer traffic, giving the SA Power Networks team peace of mind that their alerts wouldn't impact customer access.

Additionally, in 2022, new regulations as part of the federal government's SOCI (Security of Critical Infrastructure) Act placed obligations on SA Power Networks as a National Critical Infrastructure Organization. In order to meet these requirements, SA Power Networks needed a comprehensive solution to help work to secure customer access to power, and protect customer data. With added regulatory obligations, the team was able to get the support they needed internally to kickstart a new cyber defense strategy to avoid not only attacks, but also fines.

Deployment

Imperva Application Security: Seamless integration meets fortified defense

As attacks against APIs were increasing in the region, SA Power Networks realized that it would need to implement extra cybersecurity precautions. When a large Australian company was breached, the team conducted research as to what allowed for the attack to happen: exposed APIs. To avoid being susceptible to such an attack, SA Power Networks evaluated its current technologies to determine if any existing tools could help secure API endpoints against excessive data exposure. Having gained confidence in Imperva Cloud WAF, SA Power Networks looked to Imperva to further help to protect its APIs. Conducting a Proof of Concept (POC) for Imperva API Security was a simple process that was triggered from the Cloud WAF management console. The POC began a thorough discovery and classification process, evaluating SA Power Networks' vulnerabilities and establishing required safeguards.

Through automatic detection and classification of API endpoints, Imperva API Security for Cloud WAF enables comprehensive API visibility for security teams – without requiring development to publish APIs via OpenAPI or by adding resource-intensive workflow to the CI/CD processes – by providing full contextual data and tags and automatically helping to determine risks around sensitive data.

SA Power Networks found that Imperva API Security was what they needed in order to close the gap in sensitive data leakage. "One of the good things about Imperva is that if an API was unauthenticated, it told you what it was missing and how you could fix it. We got the POC running, it came in, it returned a list of a few endpoints that were unauthenticated, and then that allowed us to take it back to the relevant teams, application teams, support teams, and get that sorted. Also, moving forward, we have a baseline in place to prevent these kinds of things from happening down the line," said Nikil Kathiravan, Cybersecurity Specialist at SA Power Networks.

"In terms of we're all going to experience a bad day, what you do on that bad day and then how you communicate that after has been a really positive experience for us with Imperva."

Nathan Morelli
Head of Cybersecurity
and IT Resilience
SA Power Networks

Results

Enhanced visibility helps to block DDoS attacks and secure API endpoints

During a relentless 3-day DDoS attack, Cloud WAF deflected approximately 18.5 million malicious attempts aimed at SA Power Networks digital infrastructure. By filtering malicious traffic, Imperva prevented service disruption and allowed SA Power Networks to maintain operations, uninterrupted, despite the day's long attack, helping to ensure customer access to power. "We don't have to turn around and say, you know what? We need to change WAFs because they didn't save the day. We say we need to keep this WAF because Imperva saved the day," said Morelli.

Beyond Cloud WAF, Imperva provides SA Power Networks with visibility into its API endpoints, spotlighting potential vulnerabilities. Having this visibility isn't only about defense, it also allows SA Power Networks to take proactive measures to secure sensitive data and prevent unauthorized access in order to keep the grid up and running. Imperva API Security also aligns with SA Power Networks DevSecOps practices, allowing the company to bolster its security while promoting agile development and deployment practices. "Having API security, I think from my perspective, is a safety blanket in a way. To know, oh yeah, if something does come up, we have an alert for it—we'll deal with it," said Lindbergh Caldeira, Head of Cybersecurity Operations at SA Power Networks.

> **"One of the good things about Imperva is that if an API was unauthenticated, it told you what it was missing and how you could fix it."**
>
> **Nikil Kathiravan**
> Cybersecurity Specialist
> SA Power Networks